ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

Survey of DOS Defense Mechanisms

Anup Ranekar[1], A. R. Bhagat Patil[2]

PG Student, Dept. of Computer Technology, Yeshwantrao Chavan College of Engineering, Nagpur (MS), India[1]

HOD, Dept. of Computer Technology, Yeshwantrao Chavan College of Engineering, Nagpur (MS), India[2]

ABSTRACT: The Denial of Service (DOS) attacks hinder the availability of service to the genuine client from the server. The DOS attacks can cause severe damage to the interconnected systems such as web servers, database servers, cloud computing servers, etc. This paper surveys the different defense mechanisms available for the denial of service attacks.

KEYWORDS: Denial of Service (DOS), defense mechanisms, network security

I. INTRODUCTION

The network security is major concern in today's world of interconnected networks. Attack on one node can cause severe impact on other nodes in a network thereby forcing network traffic to behave abnormally. Different types of attacks are experienced by the server frequently that hampers the performance of server in the network. Denial of Service attack (DOS) is one of the most difficult issues to address. In DOS attacks, the attackers consume all of the computing or communicating resources that are required to provide the internet services. They misguide the server by appearing as a legal entity in the network. The attackers require a very few resources and bandwidth for execution. Such DOS attacks can bring down a web server irrespective of its hardware capabilities. Unfortunately, as a result, the legitimate users could not get the services they needed from the server. Hence it is important to inspect the network traffic for the malicious or infected packets. The malicious packets should be separated from the normal ones in order to make services available to the legitimate users or clients. Various defense mechanisms for DOS attacks are proposed. The brief overview of defense mechanisms is given in the next section.

II. DEFENSE MECHANISMS SURVEY

The DOS defense mechanism uses various approaches to tackle the DOS attacks. Some of the approaches are surveyed are as follows:
Denial of Service attacks on servers is the major concern of network security in today's world. The DOS attacks aims at the HTTP request of the clients. The traffic sampling is a technique that bifurcate the network traffic on the basis of parameters such as number, average length of flow, identifying the traffic of interest, etc. Jianpeng Zhao, Shize Guo, Kangfeng Zheng, Xinxin Niu, Yao Jiang [1] use traffic sampling which samples arrived HTTP requests and registers the information of traffic characteristics by scheduled rules. The information such as source IP, source port, destination IP, destination port, protocol type, start and end time of the HTTP request packet is registered. With the help of the registered information the attacking traffic is classified by measuring the accessing time content. Zhiyuan Tan, Aruna Jamdagni, Xiangjian He, Priyadarsi Nanda, Ren Ping Liu [9] uses Multivariate Correlation Analysis (MCA) for accurate network traffic characterization by extracting the geometrical correlations between network traffic features. Sample-by-sample detection method is used for tackling the DOS attacks. Moreover the traffic can behave false-positive or false-negative to confuse the server, need to detect and mitigate such type of behavior of network traffic. Huizhong Sun, Wingchiu Ngan, H. Jonathan Chao [3] proposes a Rateguard system that deals with such types of attacks based on leaky-bucket based rate control technique. Cornel Barna, Mark Shtern, Michael Smit, Vassilios Tzerpos, Marin Litoiu [25] use false-positive and false-negative rates for mitigating the model-based attacks.

Authentication is one of the major issues for the server to decide the legitimate user. Client puzzles helps server for authentication and association. Server sends the puzzle to the requesting client, after solving the puzzle successfully client is able to access the services on the server. The puzzle should be time dependent so that client can get only limited time to solve it. Zhang Laishun, Zhang Minglei, GuoYuanbo [4] proposes a lightweight mechanism to defend against DoS attacks on 802.11 networks. Client puzzles are implemented on the access points in WLAN's in order to

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

defend the resource depletion attacks. Yaohui Lei, Samuel Pierre, Alejandro Quintero [5] proposes client puzzles based on partial collisions in hash functions. Due to which the fine-grained control over the puzzles is possible which is useful for the access control. Mudhakar Srivatsa, Arun Iyengar, Jian Yin and Ling Liu [26] proposed a client transparent technique. They embedded an authentication code in the port number field of TCP packet and used IP level filtering to counter the DOS attacks.

The DOS attacks also aims at the TCP, ICMP, UDP, etc. Mostly the flood attacks are sent on them. Thresholds are used to detect such type of flood attacks and defend against them. Alberto Compagno, Mauro Conti, Paolo Gasti, Gene Tsudik [6] proposes a Poseidon framework which mitigates the distributed denial of service attacks. Interest flooding in named data networks (NDN) which exploits the key architectural features of NDN is mitigated by setting up the threshold which limits the rate of incoming interests from the interface. Chin-Ling Chen, Chih-Yu Chang [8] implements a two-tier coordinated defense scheme against distributed denial of service attacks which uses flood detection by threshold and online monitoring is done. Katerina Argyraki and David R. Cheriton [41] presented a network layer defense against internet bandwidth flood attacks. They propose an AITF protocol which does the network layer filtering and effectively tackles the flooding attacks. Yu Ming [43] also proposed a defense mechanism for SYN flooding attacks. He calculated the probabilities of establishment of successful connections and builds an analytical model that drops the flood based on the calculated probabilities. Vahid Aghaei Foroushani and A. Nur Zincir-Heywood [49] uses the spoofed IP addresses for their trace back based defense mechanism against the DDOS flooding attacks. Tian Zhihong, Jiang Wei, Wu Zhen and Zou Xin [47] used the rate limiter scheme for defending the DDOS attacks. Cliff C. Zou, Nick Duffield, Don Towsley and Weibo Gong [30] presented an adaptive defense system against the SYN flood DDOS attack. Hop count filtering is used for mitigating the SYN flood DDOS attack. Also they used probabilistic marking against internet worm infection.

Packet fields are used to inspect the malicious packets and also the flow table can be generated from the packets to handle the incoming attacks from the hacker. Jalal Atoum, Omar Faisal [11] uses packet reflector and a graveyard that drops the malicious packets after confirming through the detection analysis and traffic controlling phases. Ahmad Sanmorino, Setiadi Yazid [12] uses the flow pattern of the packets to mitigate the DDoS attacks. Ritu Maheshwari, Dr. C. Rama Krishna, Mr. M. Sridhar Brahma [13] uses a DPHCF-RTT technique which is probability-based packet filtering technique against IP spoofing based distributed DOS attacks. Biswa Ranjan, Swain and Bibhudatta Sahoo [23] uses more probabilistic approach for mitigating distributed DOS attacks based on TTL hop count filtering. Bharathi KrishnaKumar, P. Krishna Kumar, Prof. Dr. R. Sukanesh [17] hop count based packet processing approach to counter the DDos attacks. Changwang Zhang, Jianping Yin, and Zhiping Cai [2] proposed a Resilient SFB (RSFB) algorithm against spoofing DDoS attacks. Moreover Linlin Qin, Yong-ping Zhang, Qing Chang [18] employed a probabilistic packet marking and deterministic packet marking schemes for defense mechanisms. Ashok Singh Sairam, Ashish Subramaniam and Gautam Baruaand [40] proposed a single packet filtering technique that is based on DERM (deterministic edge marking). For providing the authentication for secure transmission of the information, hash chains are used. Ruiliang Chen, Jung-Min Park and Randolph Marchany [36] proposed a defense mechanism based on divide and conquer strategy for the DDOS attacks. They implemented a model that uses both pushback and packet marking concepts.

Network processor's ability to process the large number of network traffic can be used to control the network traffic. Li Xinlei, Zheng Kangfeng and Yang Yixian [45] used the same concept and proposed the defense scheme based on the network processor. The mechanism utilizes the processing ability of network processor to divide traffic into the different types and then uses QoS mechanism for stable communication. Thomas Dubendorfer, Matthias Bossardt and Bernhard Plattner [31] used the capability of network traffic processing device and proposed an adaptive distributed traffic controlling system for mitigating the DDOS attacks.

The DDoS attacks are more serious and to respond to this threat it is important to test and evaluate such attacks. Testbeds can be used for the testing and evaluation of DDoS attacks. Song Ning, Qiu Han [19] describes the design and implementation of DDoS attack defense testbed. OPNET and VMware workstation are used in co-simulation for the attacking and defending method. B.S. Kiruthika Devi, G. Preetha, S. Mercy Shalinie [20] proposed an Interface Based Rate Limiting (IBRL) algorithm that mitigates the DDoS attacks. The implementation is carried out on an experimental testbed build up on Linux machines and Virtual routers.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

Routers can be used in order to mitigate the DOS attacks far from the server so the network traffic cannot grow at the server end. D. Yau, J. Lui, and F. Liang [16] proposed a router throttle mechanism which is installed at the routers that are close to the victim. These routers proactively regulate the incoming packets to a moderate level, thus reducing the amount of the flooding traffic toward the victim. Haining Wang and Kang G. Shin [21] proposes a protection mechanism based on transport aware routers. A fine grained quality of service (QoS) classifier is used that effectively reduces the vulnerability of DDoS attacks by differentiation and isolation of the resources. Md. Khamruddin and Dr Ch. Rupa [37] proposed a rule –based DDOS mitigation scheme that uses the upstream routers. The upstream routers are used to control the network traffic. They focus on forwarding the normal traffic to the legitimate machines and drop the abnormal traffic. Nam-Seok Ko, Sung-Kee Noh, Jong-Dae Park, Soon-Seok Lee and Hong-Shik Park [32] proposed an anti-DDOS mechanism. They added an authorization flag to the flow state information and control the traffic according to authorization status in a flow based routing.

IP traceback technique can be used in order to defend the DOS attacks. Most of the IP traceback techniques are proposed are based on packet marking and logging. S. Malliga and Dr. A. Tamilarasi [38] presented a deterministic packet marking scheme that keeps track of the routers in the network that involved in the packet forwarding and marks them with modulo division. This scheme needs very low packet logging. Yang Xiang and Wanlei Zhou [46] used a large scale IP traceback defense mechanism system. They proposed a flexible deterministic packet marking as a countermeasure for the DDOS attacks. Schedulling can be used to mitigate the DOS attacks. Euijin Choo, Heejo Lee and Wan Yeon Lee [39] proposed a defense mechanism for motion based DOS attacks. They used dynamic multimedia scheduling scheme. The multimedia applications with multiple queues are also handled by two queue schedulers.
Fei Wang, Xiaofeng Hu, Xiaofeng Wang, Jinshu Su and Xicheng Lu [27] analyzed the traffic patterns and their relationship with the DDOS attacks. Depend on this analysis, they estimate traffic aggregates and used them for unfair rate limiting against DDOS attacks. Nen-Fu Huang, Chia-Nan Kao, Hsien-Wei Hun, Gin-Yuan Jai and Chia-Lin Lin [28] used data mining for in-depth network security. They employed data mining for analyzing the alerts from the system and accordingly they set thresholds to counter the DDOS attacks. Xiaosong Lou, Kai Hwang and Yue Hu [29] proposed an AIP protocol to tackle the DDOS attacks in peer to peer networks. They enhanced the file indexing with peer accountability to defend the index poisoning attacks.

Security in virtual networks is an important issue. Chun-Jen Chung, Pankaj Khatkar, Tianyi Xing, Jeongkeun Lee and Dijiang Huang [10] proposes a intrusion detection system that uses virtual topology attack graphs to counter the attacks in clouds. On the basis of attack graphs the countermeasures can be created in terms of cost, intrusiveness and effectiveness. Jerome Francois and Issam Aib [22] uses a FireCol mechanism for detecting the attacks and proposed the virtual protection shields for mitigating the attacks by blocking the attack related source IP's.

Many address-switch protocols are presented for limiting the effectiveness of DOS attacks. Shim6 is one example of such address switching protocols. Xiangbin Cheng, Jun Bi and Xing Li [42] proposed a swing defense mechanism based on shim6. As soon as the malicious traffic is detected, the server automatically changes its address. False data injection attacks can prove fatal to the systems which are related to the security. Suzhi Bi and Ying Jun(Angela) Zhang [48] presented graphical methods for the false injection attacks. They implemented the algorithms based on variant Steiner tree. Qingyu Yang, Jie Yang, Wei Yu, Dou An, Nan Zhang and Wei Zhao [50] proposed spatial and temporal based detection schemes for false data injection attacks. Markus Goldstein, Christoph Lampert, Matthias Reif, Armin Stahl and Thomas Breuel [33] used history based IP filtering. They used Bayes optimal filtering of network packets to mitigate the DDOS attacks.

Mohit Mehta, Kanika Thapar, George Oikonomou and Jelena Mirkovic [34] combined two defense systems: Speak-up and DefCOM to countermeasure the DDOS attacks. Wei Ren, Hai Jin and Tenghong Liu [35] proposed defense scheme for mobile ad-hoc networks. They used packet receiving frequency, channel sensing busy frequency and retransmission times for detecting the abnormal packets and then they are dropped according to the threshold. It is the era of 3G cellular networks. New network architecture are designed and implemented efficiently. These new networks are susceptible to a new kind of DOS attacks. Zhizhong Wu, Xuehai Zhou and Feng Yang [44] proposed a randomization method for such type of attacks. They focused on the DOS signaling attacks by implying a randomization degree into the architecture of 3G networks.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

III. CONCLUSION

The defense mechanisms for DOS attacks are reviewed in the literature review section. Some of them are good for direct attack, some of them are good of protocol attack, some of costly, or some of them complex or difficult in implantation. More efficient mechanisms can be built in terms of performance and time.

REFERENCES

1. Jianpeng Zhao, Shize Guo, Kangfeng Zheng, Xinxin Niu, Yao Jiang, "An Active Defense Model for Web Accessing Dos Attacks", IEEE International Conference on Information Theory and Information Security (ICITIS), 2010.
2. Changwang Zhang, Jianping Yin, and Zhiping Cai, "RSFB: a Resilient Stochastic Fair Blue algorithm against spoofing DDoS attacks", 9th International Symposium on Communications and Information Technology (ISCIT), 2009.
3. Huizhong Sun, Wingchiu Ngan, H. Jonathan Chao, "RateGuard: A Robust Distributed Denial of Service (DDoS) Defense System", IEEE Global Telecommunications Conference, 2009.
4. Zhang Laishun, Zhang Minglei, GuoYuanbo, "A Client Puzzle Based Defense Mechanism to Resist DoS Attacks in WLAN", International Forum on Information Technology and Applications, 2010.
5. Yaohui Lei, Samuel Pierre, Alejandro Quintero, "Client Puzzles Based on Quasi Partial Collisions Against DoS Attacks in UMTS", IEEE 64th Vehicular Technology Conference, 2006.
6. Alberto Compagno, Mauro Conti, Paolo Gasti, Gene Tsudik, "Poseidon: Mitigating Interest Flooding DDoS Attacks in Named Data Networking", 38th Annual IEEE Conference on Local Computer Networks, 2013.
7. Zeng Xiao-hui, Peng Xuan-ge, Li Man-hua, Xu Hong-qi, Jin Shi-yao, "Research on An Effective Approach against DDoS Attacks", International Conference on Research Challenges in Computer Science, 2009.
8. Chin-Ling Chen, Chih-Yu Chang, "A Two-Tier Coordinated Defense Scheme against DDoS Attacks", IEEE International Conference on Computer Science and Service System (CSSS), 2011.
9. Zhiyuan Tan, Aruna Jamdagni, Xiangjian He, Priyadarsi Nanda, Ren Ping Liu, "A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis", IEEE Transactions on parallel and distributed systems,2013.
10. Chun-Jen Chung, Pankaj Khatkar, Tianyi Xing, Jeongkeun Lee, Dijiang Huang, "NICE: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems", IEEE transactions on dependable and secure computing, vol. 10, no. 4, 2013.
11. Jalal Atoum, Omar Faisal, "Distributed Black Box and Graveyards Defense Strategies Against Distributed Denial of Services", Second International Conference on Computer Engineering and Applications, 2010.
12. Ahmad Sanmorino, Setiadi Yazid, "DDoS Attack Detection Method and Mitigation Using Pattern of the Flow", International Conference of Information and Communication Technology (ICoICT), 2013.
13. Ritu Maheshwari, Dr. C. Rama Krishna, Mr. M. Sridhar Brahma, "Defending Network System against IP Spoofing based Distributed DoS attacks using DPHCF-RTT Packet Filtering Technique", IEEE Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014.
14. Monika Sachdeva, Gurvinder Singh, Krishan Kumar, "An Emulation Based Impact Analysis of DDoS Attacks on Web Services during Flash Events", International Conference on Computer & Communication Technology (ICCCT), 2011.
15. Shui Yu, Yonghong Tian, Song Guo, Dapeng Oliver Wu, "Can We Beat DDoS Attacks in Clouds?", IEEE Transactions on parallel and distributed systems, 2013.
16. D. Yau, J. Lui, and F. Liang, "Defending against Distributed Denial-of-Service Attacks with Max-Min Fair Server-Centric Router Throttles", Proc. Internationall Workshop Quality of Service, May 2002.
17. Bharathi KrishnaKumar, P.Krishna Kumar, Prof. Dr. R. Sukanesh, "Hop Count Based Packet Processing Approach to Counter DDoS Attacks", International Conference on Recent Trends in Information, Telecommunication and Computing, 2010.
18. Linlin Qin, Yong-ping Zhang, Qing Chang, "A Novel Improved Compositive DDoS Defence System", 2nd International Conference on Signal Processing Systems (ICSPS), 2010.
19. Song Ning, Qiu Han, "Design and Implementation of DDOS attack and Defense Testbed", IEEE International Conference on Wavelet Active Media Technology and Information Processing (ICWAMTIP), 2012.
20. B.S. Kiruthika Devi, G. Preetha, S. Mercy Shalinie, "DDoS Detection using Host-Network based Metrics and Mitigation in Experimental Testbed", International Conference on Recent Trends In Information Technology (ICRTIT), 2012.

Haining Wang, Kang G. Shin, "Transport-Aware IP Routers: A Built-In Protection Mechanism to Counter DDoS Attacks", IEEE Transactions on Parallel and Distributed Systems, 2003.

21. Jerome Francois, Issam Aib, "FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks", IEEE/ACM Transactions on networking, vol. 20, 2012.
22. Biswa Ranjan, Swain, Bibhudatta Sahoo, "Mitigating DDoS attack and Saving Computational Time using a Probabilistic approach and HCF method ", IEEE International Advance Computing Conference (IACC), 2009.
23. Moti Geva, Amir Herzberg, Yehoshua Gev, "Bandwidth Distributed Denial of Service: Attacks and Defenses", IEEE Conference on Communications and Network Security, 2013.
24. Cornel Barna, Mark Shtern, Michael Smit, Vassilios Tzerpos, Marin Litoiu, "Model-Based Adaptive DoS Attack Mitigation", ICSE Workshop on Software Engineering for Adaptive and Self-Managing Systems , 2012.
25. Mudhakar Srivatsa, Arun Iyengar, Jian Yin, Ling Liu, "A Client-Transparent Approach to Defend Against Denial of Service Attacks", 25th IEEE Symposium on Reliable Distributed Systems, 2006.
26. Fei Wang, Xiaofeng Hu, Xiaofeng Wang, Jinshu Su, Xicheng Lu, "Unfair rate limiting on traffic aggregates for DDoS attacks mitigation", IET International Conference on Information Science and Control Engineering (ICISCE) 2012.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

27. Nen-Fu Huang, Chia-Nan Kao, Hsien-Wei Hun, Gin-Yuan Jai, Chia-Lin Lin, "Apply Data Mining to Defense-in-Depth Network Security System", 19th International Conference on Advanced Information Networking and Applications (AINA), 2005.
28. Xiaosong Lou, Kai Hwang, Yue Hu, "Accountable File Indexing against DDoS Attacks in Peer-to-Peer Networks", IEEE Global Telecommunications Conference (GLOBECOM), 2009.
29. Cliff C. Zou, Nick Duffield, Don Towsley, Weibo Gong, "Adaptive Defense Against Various Network Attacks",IEEE Journal on Selected Areas in Communications, 2006.
30. Thomas Dubendorfer, Matthias Bossardt, Bernhard Plattner, "Adaptive Distributed Traffic Control Service for DDoS Attack Mitigation", 19th IEEE International Parallel and Distributed Processing Symposium, 2005.
31. Nam-Seok Ko, Sung-Kee Noh, Jong-Dae Park, Soon-Seok Lee, Hong-Shik Park, "An Efficient Anti-DDoS Mechanism using Flow-based Forwarding Technology", 9th International Conference on Optical Internet (COIN), 2010.
32. Markus Goldstein, Christoph Lampert, Matthias Reif, Armin Stahl, Thomas Breuel, "Bayes Optimal DDoS Mitigation by Adaptive History-Based IP Filtering", Seventh International Conference on Networking (ICN), 2008.
33. Mohit Mehta, Kanika Thapar, George Oikonomou, Jelena Mirkovic, "Combining Speak-up with DefCOM for Improved DDoS Defense", IEEE International Conference on Communications (ICC), 2008.
34. Wei Ren, Hai Jin, Tenghong Liu, "Congestion Targeted Reduction of Quality of Service DDoS Attacking and Defense Scheme in Mobile Ad Hoc Networks",Seventh IEEE International Symposium on Multimedia, 2005.
35. Ruiliang Chen, Jung-Min Park, Randolph Marchany, "A Divide-and-Conquer Strategy for Thwarting Distributed Denial-of-Service Attacks", IEEE Transactions on Parallel and Distributed Systems, 2007.
36. Md. Khamruddin, Dr Ch. Rupa, "A Rule Based DDoS Detection and Mitigation Technique", Nirma University International Conference on Engineering (NUiCONE), 2012.
37. S.Malliga, Dr. A.Tamilarasi, "A defensive mechanism to defend against DoS/DDoS attacks by IP traceback with DPM", International Conference on Computational Intelligence and Multimedia Applications, 2007.
38. Euijin Choo, Heejo Lee, Wan Yeon Lee, "Dynamic Multimedia Scheduling against Motion based DoS Attacks", International Conference on Information Networking (ICOIN), 2009.
39. Ashok Singh Sairam, Ashish Subramaniam, Gautam Baruaand, "Defeating Reflector Based Denial-of-Service Attacks using Single Packet Filters", 5th International ICST Conference on Communications and Networking in China (CHINACOM), 2010.
40. Katerina Argyraki, David R. Cheriton, "Scalable Network-Layer Defense Against Internet Bandwidth-Flooding Attacks", IEEE/ACM Transactions on Networking, 2008.
41. Xiangbin Cheng, Jun Bi, Xing Li, "Swing - A Novel Mechanism Inspired by Shim6 Address-Switch Conception to Limit the Effectiveness of DoS Attacks", Seventh International Conference on Networking (ICN), 2008.
42. Yu Ming, "A Probabilistic Drop Scheme for Mitigating SYN Flooding Attacks", International Conference on Networks Security, Wireless Communications and Trusted Computing (NSWCTC), 2009.
43. Zhizhong Wu, Xuehai Zhou, Feng Yang, "Defending against DoS Attacks on 3G Cellular Networks Via Randomization Method", International Conference on Educational and Information Technology (ICEIT), 2010.
44. Li Xinlei, Zheng Kangfeng, Yang Yixian, "A DDoS attack defending scheme based on network processor", WASE International Conference on Information Engineering (ICIE), 2009.
45. Yang Xiang, Wanlei Zhou, "A Defense System Against DDoS Attacks by Large-Scale IP Traceback", Third International Conference on Information Technology and Applications (ICITA), 2005.
46. Tian Zhihong, Jiang Wei, Wu Zhen, Zou Xin, "A Game Theory based Rate Limiting Scheme against Distributed Denial-of-Service Attacks", The 2nd IEEE International Conference on Information Management and Engineering (ICIME), 2010.
47. Suzhi Bi, Ying Jun(Angela) Zhang, "Graphical Methods for Defense Against False-Data Injection Attacks on Power System State Estimation", IEEE Transactions on Smart Grid, 2013.
48. Vahid Aghaei Foroushani, A. Nur Zincir-Heywood, "TDFA: Traceback-based Defense against DDoS Flooding Attacks", 28th IEEE International Conference on Advanced Information Networking and Applications (AINA), 2014.
49. Qingyu Yang, Jie Yang, Wei Yu, Dou An, Nan Zhang, Wei Zhao, "On False Data-Injection Attacks against Power System State Estimation: Modeling and Countermeasures", IEEE Transactions on Parallel and Distributed Systems, 2013.